



Transparency Best Practices for Schools and Districts

About PTAC

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a “one-stop” resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available on <http://ptac.ed.gov>.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Why is Transparency Important?

Schools and districts across the country need to collect data about students, including their test scores, grades, credits earned, and other related information, such as demographics, enrollment, discipline, and special education status. Educational agencies and institutions use these data to foster students’ academic achievement by identifying students’ talents and special requirements, monitoring their academic progress, and developing successful teaching and learning strategies. Schools and districts often have legitimate educational reasons to authorize third-parties to access these student data, for purposes such as communicating with parents, improving the effectiveness of education programs, to identify gaps in student services, and reasons as simple as providing secure data storage.

Parents expect their children’s well-being to come first when children attend school. This includes the expectation of respect for students’ privacy and adequate protection of the confidentiality of children’s personal information. To that end, parents expect openness and transparency from schools and districts about their data practices, so that parents can evaluate whether a school’s or district’s protection of children’s personal information meets those expectations.

Consequently, it is important that schools and districts communicate what student information they collect, why they collect it, how they use it, and to whom they disclose it. The U.S. Department of Education (ED or Department) encourages schools and districts to take a proactive approach in communicating with parents, as greater understanding of the schools’ and districts’ data privacy policies and practices will help alleviate confusion and misunderstandings about students’ data use.

This document is intended to assist elementary and secondary schools and local educational agencies (LEAs or “districts”) in achieving greater transparency with respect to their data practices. It informs

schools and districts of the basics of legal compliance, but encourages educational organizations as a best practice to go beyond the minimum notifications required under federal law. While the primary intended audience for this document is K-12 institutions and agencies, many of the recommendations apply equally to educational organizations at other levels.

Required Privacy Rights Notifications (FERPA and PPRA)

To maximize transparency, ED encourages schools and districts to share certain information with parents as a best practice. Before discussing best practices, however, we will first briefly describe the requirements under federal law for what information **must** be provided to parents and students.

FERPA

The Family Educational Rights and Privacy Act (FERPA), a federal law administered by the Department (20 U.S.C. § 1232g; 34 CFR Part 99), affords parents and “eligible students” (students who are at least 18 years old, or, in attendance at a postsecondary institution at any age) certain rights with respect to education records, such as the right to consent to the disclosure of personally identifiable information (PII) from the education records (except in certain circumstances).

FERPA requires schools and districts to provide annual notification to parents and eligible students of their rights under FERPA, including:

- the right to inspect and review their education records, the right to seek to amend those records, the right to consent to disclosure of PII from those records (unless an exception applies), and the right to file a complaint with the Department regarding an alleged FERPA violation;
- the procedure for exercising the right to inspect and review education records, and the procedure for requesting amendment of those records; and
- the school’s or district’s criteria for determining who constitutes a “school official” and what constitutes a “legitimate educational interest.”

Additionally, if a school or district has a policy of disclosing “directory information” under FERPA, it must provide public notice to parents and eligible students of that policy. “Directory information” means information about a student that would not generally be considered harmful or an invasion of privacy if disclosed, such as name, address, and telephone number; many schools adopt directory information policies in order to include this information in yearbooks, concert programs, student/parent directories, etc. (See 34 CFR § 99.3 “Directory information” for additional examples of data elements commonly designated as directory information). If a school or district elects to disclose directory information, the directory information notice must include:

- the types of PII that the district or school has designated as directory information;
- an explanation of the right of parents and eligible students to request that the information about the student not be disclosed as directory information;

- a specified period of time within which a parent or eligible student may notify the school or LEA in writing that they do not want any or all of the information disclosed as directory information. (There are two exceptions to the ability to opt out set forth in § 99.37(c).); and
- (optional) if the school or district has chosen to adopt a “limited directory information policy,” the limited parties or purposes for which directory information may be disclosed. (See <http://www.ed.gov/fpco> for more information on limited directory information policies.)

The school or district may also want to include in the annual notification that it routinely discloses students’ education records to other schools in which the student seeks or intends to enroll.

PPRA

In many instances, schools or districts must also provide notice under the Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h; 34 CFR Part 98), another federal law that applies to recipients of funds under any program administered by the Department. The PPRA only applies to elementary and secondary schools (not to higher education institutions), and addresses, among other matters, the use of personal information collected from students for marketing purposes, and the administration of certain surveys and evaluations to students.

Subject to limited exceptions, the PPRA requires a school or district that receives funds under any applicable Department program to develop and adopt certain policies in consultation with parents, and to provide parents with notice of those policies and their rights under PPRA at least annually (at the beginning of the school year), and within a reasonable period of time after any substantive change is made to those policies. The complete PPRA requirements regarding these policies, and the instances in which direct notification is required, can be found at 20 U.S.C. § 1232h(c)(1-2), and the exceptions to these requirements can be found at 20 U.S.C. § 1232h(c)(4).

For additional information about required notices under FERPA and PPRA, please visit the Family Policy Compliance Office (FPCO) website, at <http://www.ed.gov/fpco>.

Best Practice Recommendations for Improving Transparency

Beyond FERPA and PPRA notification requirements, the Department recommends a number of best practices for improving the transparency of schools’ and districts’ data practices. These recommendations can be divided into three main categories: (1) what information to communicate to parents; (2) how to convey that information; and (3) how to respond to parent inquiries about student data policies and practices.

Recommendations on What to Communicate to Parents:

In addition to the mandatory information outlined above that schools and districts are legally required to include in notices to parents and eligible students, as a best practice also provide

parents with the following information about your school's or district's data and privacy practices:

- ☑ *What information are you collecting about students?*
 - Develop and publish a data inventory listing the information that you collect from or about your students. A best practice is to provide this information at the data element level.
 - **REMEMBER:** The first step in protecting sensitive information is knowing what information you have.

- ☑ *Why are you collecting this information?*
 - Explain why you collect student information (e.g., for state or federal reporting, to provide educational services, to improve instruction, to administer cafeteria services, etc.). A best practice is to provide this information at the data element level.
 - **REMEMBER:** If you cannot provide a good reason for why you are collecting a particular data element, you may want to reconsider collecting it.

- ☑ *How is the information protected?*
 - Explain your institution's information technology (IT) security and data protection policies (both for paper records and for digital information).
 - Describe your school's or district's policies governing access and use of students' PII.
 - Explain your data retention policies, and whether you retain records in identifiable, minimized/redacted, or de-identified form. (See "[Minimizing Access to PII: Best Practices for Access Controls and Disclosure Avoidance Techniques](#).")
 - If you publish aggregate data on your website (or if you provide it to the media or the general public), explain the privacy protections you apply to protect against disclosure of students' PII in "small cells." (See "[Frequently Asked Questions—Disclosure Avoidance](#).")
 - **REMEMBER:** It is important to regularly train your faculty and staff on these IT security and data protection policies.

- ☑ *Do you share any personal information with third parties? If so, with whom, and for what purpose(s)?*
 - If you contract for services that require you to share student information, consider posting those contracts online.
 - Provide parents with a list of online educational services or "apps" that are approved for use in the classroom.
 - If you share student information with external researchers (e.g., under FERPA's "studies" or "audit and evaluation" exceptions – see "[FERPA Exceptions Summary](#)"), show parents the research findings and identify if you made any changes to curriculum, policies, or programs as a result.
 - **REMEMBER:** Parents care about who has access to and uses their children's information. Let them know the reasons you are sharing student data with a third party and explain the legal, contractual, and policy protections in place to safeguard the data.

- ☑ *Who should parents contact if they have questions about your data practices?*
 - Display contact information prominently on your website, so that it is clear whom parents can contact if they have questions, comments, or suggestions.
 - **REMEMBER:** Posting information on a website is not enough—ask for constructive feedback from parents and students to ensure that the policies and practices are truly transparent.

Recommendations on How to Communicate about Data Practices:

When communicating with parents about the school’s or district’s data practices, consider the following best practices to improve accessibility and clarity of the messages:

- ☑ *Use your website as part of a multi-layered approach to communication*
 - Layer the sophistication of the message to the medium. For example, shorter documents or announcements, such as a letter to parents, student handout, newsletter item, or a blog post could contain a very simple message, supplemented by a link to additional, more in-depth information for those who are interested.
 - Post electronic copies of your required FERPA and PPRA notices on your website as a reference for parents and students to consult later.

- ☑ *Make your website user-friendly, searchable, and easy to navigate*
 - When possible, consolidate information about data practices and privacy protections into a single page or section on your website.
 - Clearly label the data practices/student privacy section and ensure that users can quickly navigate to it from the homepage with just one or two mouse clicks.
 - Add a “Search” tool to your website so that visitors can easily find relevant information on data practices using common keywords.

- ☑ *Be clear and consistent*
 - Use plain language whenever possible (avoid legal or technical jargon).
 - Provide examples to illustrate complex concepts or ideas.
 - Include a glossary with definitions and links to relevant privacy laws, regulations, or policies.
 - Make sure that your website’s data practices section is accessible to persons with disabilities.
 - Consider translating the data practices section and any related student privacy information on your website into other languages commonly spoken in your community.
 - Maintain consistency across communication mediums (i.e., between written letters and website pages).

- ☑ *Have members of the community regularly review your website for useability, comprehension, and completeness*

- Follow up with parents and students to ensure that they can easily find and understand the data and privacy practices information posted on your website.
- Solicit feedback from parents and students on recommended improvements to your website or for additional information to include about your data and privacy practices.

Recommendations for Responding to Parent Inquiries:

Sometimes parents or students will contact you wanting additional information. ED encourages schools and districts to handle parental and student inquiries about data privacy in a responsive and meaningful fashion. The best practices include:

- Keep the lines of communication open*
 - Be available to answer questions from parents and students regarding student data.
 - Provide parents and students with multiple easy ways to reach staff for questions, concerns, or suggestions.
 - Parents and students should be able to reach out for help in ways that are convenient to them.
 - When appropriate, use online systems that grant parents access to their children’s information so that parents can learn more about their children’s progress and activities in school.
- Review parental inquiries, concerns, and suggestions in a thoughtful and careful manner*
 - Don’t dismiss inquiries, concerns, or suggestions without sufficient consideration.
 - Acknowledge parents’ concerns about their child’s well-being.
 - Make the effort to properly understand the question, concern, or suggestion and relevant circumstances—follow-up to obtain additional information if necessary.
 - Respond in a clear, respectful, and meaningful fashion to minimize confusion.
- Respond to parental or student inquiries in a timely manner.*
 - Notify the parent or student about the expected turn-around time and explain the logistics of the response process; this information can be posted on the school’s or district’s website, communicated directly to the requester, or both.
 - If additional time is required to address the inquiry, follow up with the parent or student to keep him or her informed about the delay and the reason for it.
- Periodically review old inquiries and resolutions to evaluate and improve your communication and transparency efforts*
 - Evaluate your effectiveness by reviewing changes in the relevant measures over time. Some useful indicators include the number of privacy concerns, response turn-around time, and feedback from parents and students.
 - Review and modify privacy policies and procedures, including the content of privacy

notices and modes of communication, at least annually.

Additional Resources

For additional information on the topics and best practice recommendations discussed above, please visit our websites. The FPCO website provides detailed guidance on legal requirements under FERPA and PPRA, and the PTAC website provides guidance documents, trainings, checklists, frequently asked questions, and other resources relating to best practices for data privacy and security.

- Family Policy Compliance Office (FPCO), U.S. Department of Education: www.ed.gov/fpc
- Privacy Technical Assistance Center (PTAC), U.S. Department of Education: <http://ptac.ed.gov>